(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 667 173**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **90 11675**

(51) Int Cl⁵ : G 06 F 12/14

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 21.09.90.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande** : 27.03.92 Bulletin 92/13.

(56) **Liste des documents cités dans le rapport de recherche** : *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *Société dite : TELEMECANIQUE (Société Anonyme)* — FR.

(72) **Inventeur(s)** : Gardaire Gilles, Jaraudias Patrice et Tournier Yves.

(73) **Titulaire(s)** :

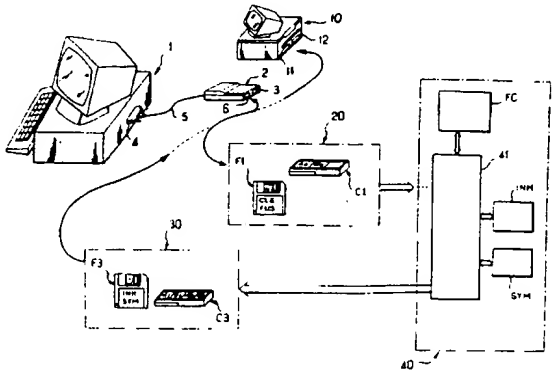
(74) **Mandataire** : Cabinet André Bouju.

(54) Procédé de protection des droits d'utilisation de plusieurs logiciels sur un poste de travail informatique ou d'automatisme industriel et système pour sa mise en œuvre.

(57) Procédé de protection des droits d'utilisation d'un ou plusieurs logiciels sur un poste de travail informatique (1, 10), ces droits étant contenus dans un module clé de travail (C1, C3) destiné à coopérer avec le poste de travail (1, 10) pour autoriser une continuité d'exploitation desdits logiciels.

Le procédé comprend, en cas de panne du module clé de travail (C1), une phase de contrôle de la détention effective des droits (A0, B0) dont la restitution est demandée, ledit module clé de travail (C1) et chacun desdits droits d'utilisation (A0, B0) étant initialement associé respectivement à un identificateur de clé et à des identificateurs de droit d'utilisation et comprend en outre, au cours de toute exécution de l'un au moins desdits logiciels ou transaction portant sur lesdits droits d'utilisation, une opération d'enregistrement de l'identificateur de clé et des identificateurs de droit d'utilisation dans au moins un fichier prédéterminé (CLE, FUS) accessible sur le poste de travail (1, 10) et transmis avec le module clé de travail défaillant.

Utilisation dans le domaine de la protection de logiciels en informatique industrielle.



FR 2 667 173 - A1

La présente invention concerne un procédé de protection des droits d'utilisation d'un ou plusieurs logiciels sur un poste de travail informatique ou d'automatisme industriel.

Elle vise également un système pour sa mise en oeuvre.

La demande de brevet français n° 90 06112 du 16 mai 1990 au nom du présent déposant divulgue un procédé de configuration d'un poste de travail informatique sur lequel sont implantés plusieurs logiciels à chacun desquels sont associés des droits d'utilisation respectifs contenus dans un module clé original distinct destiné à coopérer avec ce poste de travail pour autoriser une continuité d'exploitation de ce logiciel.

Ce procédé comprend une succession d'étapes de transfert, chaque étape de transfert réalisant l'union de droits contenus initialement dans deux modules clés et leur transfert dans l'un desdits modules clés, l'autre module clé étant rendu vide de tout droit, de sorte qu'à l'issue de cette succession d'étapes de transfert, on dispose d'un module clé original unique contenant l'ensemble des droits d'utilisation associés aux logiciels implantés sur le poste de travail, l'ensemble des autres modules clés étant rendus vides de tout droit.

Avec ce procédé, le problème posé par le nombre limité d'emplacements de modules clés est résolu puisqu'à l'issue d'étapes de transfert successives, un seul module clé contient l'ensemble des droits d'utilisation des différents logiciels implantés sur le poste de travail informatique.

Cependant, un problème délicat concerne la difficulté de prouver, en cas de défaillance du module clé de travail contenant une fusion de droits d'utilisation, la nature et le nombre de droits

effectivement présents au moment de la défaillance. Ceci peut avoir des conséquences économiques non négligeables pour le prestataire des logiciels dans le cas où des utilisateurs malhonnêtes demanderaient la restitution de droits d'utilisation abusivement déclarés détruits en affirmant que le module clé en panne contenait une union de droits et retourneraient au prestataire un module clé effectivement détruit mais qui, par le biais d'une opération de partition ou de transfert, aurait été au préalable vidée de tout droit.

La demande de brevet français n° 90 06112 du 16 mai 1990 au nom du présent déposant divulgue un procédé de gestion des droits d'utilisation de plusieurs logiciels sur un poste de travail informatique ou d'automatisme industriel, ces droits étant contenus dans un module clé original destiné à coopérer avec le poste de travail pour autoriser une continuité d'exploitation des logiciels.

Ce procédé de gestion comprend une étape préalable de création d'un module clé de travail et d'un module clé de sauvegarde associé de façon exclusive au module clé de travail, à partir du module clé original et d'un premier module clé vierge, suivie d'une étape d'exploitation normale des logiciels sur le poste de travail.

Avec ce procédé, l'utilisateur dispose d'un module clé de sauvegarde qui doit être placé en lieu sûr et qui est mis en oeuvre en cas de panne du module clé de travail. Ce module clé de sauvegarde étant associé de façon exclusive au module clé de travail, le prestataire des logiciels a la garantie qu'un module clé de sauvegarde contenant des droits d'utilisation différents, ne pourrait être substitué au module clé de sauvegarde créé préalablement.

Or il existe des situations où un nombre limité

d'emplacements sur le support de clés (par exemple deux) ne permet pas la mise en oeuvre d'un module clé de sauvegarde ou duplicata. Par ailleurs, il ne faudrait pas dans la mesure du possible apporter de contraintes supplémentaires pour un utilisateur honnête. En outre, le temps d'immobilisation du poste de travail en cas de panne devrait être minimisé.

Le but de la présente invention est de remédier à ces inconvénients en proposant un procédé de protection des droits d'utilisation d'un ou plusieurs logiciels sur un poste de travail informatique ou d'automatisme industriel, ces droits étant contenus dans un module clé de travail destiné à coopérer avec le poste de travail pour autoriser une continuité d'exploitation desdits logiciels.

Suivant l'invention, le procédé comprend, en cas de panne du module clé de travail, une phase de contrôle de la détention effective par l'utilisateur du poste de travail des droits dont la restitution est demandée, ledit module clé de travail et chacun desdits droits d'utilisation étant initialement associé respectivement à un identificateur de clé et à des identificateurs de droit d'utilisation, et il comprend en outre, au cours de toute exécution de l'un au moins desdits logiciels ou transaction portant sur lesdits droits d'utilisation, une opération d'enregistrement de l'identificateur de clé et des identificateurs de droit d'utilisation dans au moins un fichier prédéterminé accessible sur le poste de travail et transmis sur un support d'informations numériques avec le module clé de travail en cas de panne.

Ainsi, le prestataire des logiciels protégés est en mesure de contrôler, par la lecture du contenu du fichier transmis avec le module clé en panne, la détention effective des droits déclarés détruits, sans qu'il soit nécessaire de disposer d'un module clé

duplicata. la présence au sein du fichier transmis de l'identificateur de clé et des identificateurs de droits permet au prestataire d'avoir la garantie que l'utilisateur du module clé en panne ne demande pas la restitution de droits d'utilisation abusivement déclarés détruits.

Selon une caractéristique avantageuse de l'invention, la phase de contrôle comprend une étape de mise à jour d'un fichier client comprenant notamment les identificateurs de clé et de droit d'utilisation, une étape de mise à jour d'un fichier de déclaration contenant l'ensemble des droits d'utilisation déclarés détruits par l'ensemble des utilisateurs desdits logiciels, et une étape de préparation et de retour au client d'une part, d'un nouveau module clé de travail contenant des droits nouveaux d'utilisation des logiciels, auxquels sont associés de nouveaux identificateurs de droit, et les droits d'utilisation des logiciels, qui ont été déclarés détruits et qui sont maintenant inhibés, et d'autre part, un support d'informations numériques contenant notamment le fichier de déclaration sous une forme non accessible en lecture, en vue de charger ledit fichier sur le poste de travail.

De cette façon, le procédé selon l'invention apporte encore un degré supplémentaire de protection puisqu'il permet la diffusion au sein des sites utilisateurs d'un fichier de déclaration contenant l'ensemble des droits d'utilisation déclarés détruits par l'ensemble des utilisateurs. Cette diffusion, qui peut être massive, permet d'empêcher toute utilisation illicite de logiciels protégés à partir de droits d'utilisation qui auraient été abusivement déclarés détruits.

Par ailleurs, le fait que ce fichier de déclaration soit non accessible en lecture par

l'utilisateur à partir d'un poste de travail, garantit qu'il ne pourra être modifié et en particulier mis à jour que dans le cadre de l'exécution d'un des logiciels protégés ou d'un logiciel de gestion de droits.

Suivant un autre aspect de l'invention, le système de protection des droits d'utilisation d'un ou plusieurs logiciels sur un poste de travail informatique, ces droits étant contenus dans un module clé de travail destiné à coopérer avec le poste de travail pour autoriser une continuité d'exploitation desdits logiciels, mettant en oeuvre le procédé selon l'invention, est caractérisé en ce qu'il comprend des moyens pour contrôler la détention effective par l'utilisateur du poste de travail, de droits dont la restitution est demandée en cas de panne du module clé de travail, à partir d'informations contenues dans des fichiers prédéterminés remis par l'utilisateur sur un support d'informations numériques avec le module clé de travail défaillant, notamment un identificateur de clé associé audit module clé et des identificateurs de droits d'utilisation associés respectivement à chacun des droits d'utilisation initialement présents dans ledit module clé.

Selon un mode préféré de réalisation de l'invention, les moyens de contrôle comprennent des moyens pour mettre à jour, d'une part, un fichier client contenant notamment l'identificateur de clé et les identificateurs de droit d'utilisation, et d'autre part, un fichier de déclaration contenant l'ensemble des droits d'utilisation déclarés détruits par l'ensemble des utilisateurs desdits logiciels, des moyens pour configurer un nouveau module clé de travail contenant des droits d'utilisation des logiciels, auxquels sont associés de nouveaux identificateurs de droit, et les droits d'utilisation qui ont été déclarés détruits et qui

sont maintenant inhibés, et des moyens pour générer sur un support d'informations numériques retourné à l'utilisateur des logiciels avec le nouveau module clé de travail, le fichier de déclaration sous forme non accessible en lecture en vue de charger ledit fichier sur le poste de travail.

D'autres particularités et avantages de l'invention apparaîtront encore dans la description ci-après. Aux dessins annexés donnés à titre d'exemples non limitatifs:

la figure 1 est vue synoptique d'un mode de mise en oeuvre du procédé de protection selon l'invention;

la figure 2 est un organigramme simplifié de la phase de contrôle mise en oeuvre dans le procédé selon l'invention;

la figure 3 est un organigramme simplifié des étapes du procédé selon l'invention effectuées lors de l'exécution d'un logiciel protégé.

On va maintenant décrire une forme préférée du procédé selon l'invention en même temps que le système pour sa mise en oeuvre.

On considère, en référence à la figure 1, un poste de travail informatique, par exemple un microordinateur 1 de type compatible PC ou un poste de travail spécialisé 10, sur lequel un utilisateur exploite plusieurs logiciels protégés à chacun desquels sont associés des droits d'utilisation respectifs. Ces droits d'utilisation peuvent être fusionnés au sein d'un module clé de travail unique C1 en mettant en oeuvre le procédé de configuration qui a fait l'objet d'une demande précédente de brevet français au nom de la demanderesse. Ce module clé C1 est destiné à être inséré dans des supports de clé qui sont soit externes 2, 3, 6 dans le cas d'un microordinateur 1, soit internes 11,12 au poste de travail spécialisé 10. A titre d'exemple, un support

de clé autonome 2 comporte deux logements 3, 6 destinés à accueillir des modules clés. Il est connecté à un port d'entrées/sorties 4 par un câble de connexion.

En cas de panne du module clé de travail C1 qui peut par exemple contenir des droits d'utilisation A0, B0 associés à deux logiciels distincts, l'utilisateur du poste de travail doit retourner au prestataire des logiciels protégés le module clé de travail défaillant accompagné d'une lettre de déclaration de destruction et d'un support d'informations numériques, par exemple une disquette magnétique F1, contenant un ou plusieurs fichiers prédéterminés CLE, FUS comportant des informations représentatives du module clé de travail concerné et des droits d'utilisation effectivement présents dans le module clé de travail au moment de la défaillance du module clé de travail C1.

On va maintenant décrire les opérations d'enregistrement des identificateurs de clé et de droits d'utilisation qui constituent ces informations. Ces opérations d'enregistrement sont effectuées à l'occasion de chaque exécution d'un des logiciels protégés sur le poste de travail 1, 10 ou d'un logiciel de gestion de droits d'utilisation implanté sur le poste de travail informatique 1 et décrit en détail dans les demandes de brevet français précitées, concernant la configuration d'un poste de travail et la gestion de droits, déposées précédemment par la demanderesse.

Dans le cas de l'exécution d'un logiciel protégé, un fichier CLE contenant un identificateur de clé associé au module clé de travail actuellement utilisé est mis à jour et contient notamment un numéro de série du module clé ou identificateur de clé, des numéros de série, ou identificateurs de droits, respectifs des droits d'utilisation contenus dans le module clé, et des informations descriptives de l'opération en cours, à

savoir l'exécution du logiciel protégé. Ce fichier CLE est commun à tous les logiciels qui s'exécutent sur le même poste de travail. Il peut être lu par l'utilisateur afin d'examiner si ce fichier contient des informations relatives à un module clé en panne.

Dans le cas de l'exécution du logiciel de gestion des droits installé sur le poste de travail 1, à l'occasion de chaque opération d'union ou de partition de droits d'utilisation, le logiciel de gestion enregistre dans un fichier FUS le numéro de série du module clé de travail C1 ou identificateur de clé, les numéros de série respectifs des droits d'utilisation, ou identificateurs de droits, et des informations descriptives de l'opération en cours, par exemple, une union de droits, une partition de droits ou une lecture de contenu du module clé de travail C1. Ce fichier FUS conserve ainsi l'historique des opérations effectuées et peut être lu par l'utilisateur du poste de travail afin également d'examiner si ce fichier contient des informations relatives à un module clé de travail en panne.

A réception du couple 20 constitué par le module clé de travail en panne C1 et la disquette F1 contenant les fichiers FUS, CLE, le prestataire des logiciels met en oeuvre un système de protection 40 comportant un dispositif 41 de contrôle de la détention effective par l'utilisateur demandeur, des droits d'utilisation dont ce dernier demande la restitution. Ce dispositif de contrôle 41 peut par exemple être un microordinateur ou tout autre moyen équivalent de traitement d'informations, associé à un support de module clé. Le dispositif de contrôle 41 met à jour d'une part, un fichier client FC et d'autre part, un fichier de déclaration INH contenant l'ensemble de tous les droits d'utilisation déclarés détruits par l'ensemble des utilisateurs des logiciels fournis par le prestataire. Le dispositif de contrôle peut en outre être

associé à un fichier SYM contenant des informations descriptives de symboles en plusieurs langues, notamment des symboles commerciaux.

A l'issue des différentes étapes du procédé qui vont être décrites dans la suite, un nouveau couple 30 module clé/disquette constitué d'un nouveau module clé de travail C3 contenant de nouveaux droits d'utilisation A1, B1 et les droits déclarés détruits et désormais inhibés A'0, B'0, et d'une disquette C3 contenant le fichier de déclaration INH inaccessible en lecture et éventuellement le fichier de symboles SYM. Pour que l'utilisateur puisse de nouveau exploiter les logiciels protégés, le fichier de déclaration INH doit être chargé sur le poste de travail 1, et le nouveau module clé de travail C3 inséré dans le support de clé 2.

On va maintenant décrire, en référence à la figure 2, la succession d'étapes effectuées au sein du système de protection lorsque le couple (module clé en panne C1 contenant les droits A0, B0; fichier F1) est reçu par le prestataire. Au cours d'une première étape a, une mise à jour du fichier client FC est effectuée, ce fichier contenant:

le nom et les coordonnées exactes du client utilisateur,

la date de l'opération,

le numéro de série du module clé retourné par le client,

le numéro de série des droits d'utilisation déclarés détruits par le client.

Une seconde étape b concerne la mise à jour du fichier de déclaration INH contenant l'ensemble des droits déclarés détruits.

Ensuite, un nouveau module clé de travail C3 est configuré de façon à contenir de nouveaux droits d'utilisation A1, B1 destinés à remplacer les droits A0,

B0 déclarés détruits, et les droits d'utilisation déclarés détruits et qui sont maintenant inhibés A'0, B'0, au cours d'une troisième étape c qui comporte en outre le transfert du fichier de déclaration INH, de préférence sous forme binaire et donc non directement accessible en lecture, sur la disquette F3 qui est retournée à l'utilisateur en même temps que le nouveau module clé de travail C3.

Si l'examen du contenu des fichiers CLE ou FUS fait apparaître au cours des étapes précitées que le module clé de travail en panne était rempli de droits au maximum de sa capacité, deux nouveaux modules clé de travail sont retournés au lieu d'un dans le cas précité, chaque module clé contenant alors des paires (droit actif, droit inhibé).

Lorsque l'utilisateur effectue la réinstallation des droits nouveaux retournés par le prestataire, un processus de protection est mis en oeuvre ; les étapes essentielles de ce processus sont illustrées en figure 3.

Après insertion du nouveau module clé de travail C3 dans un support de clé connecté au poste de travail, une première étape A de lecture de tous les droits, actifs ou inhibés, contenus dans le module clé C3 est effectuée. Elle est suivie d'une mise à jour B des fichiers CLE ou FUS. Une vérification C de l'existence sur le poste de travail et de l'intégrité d'un fichier de déclaration INH, est effectuée pour prévenir des modifications anormales de ce fichier. Cette vérification est suivie d'une mise à jour du fichier à partir des informations contenues dans la disquette F3, par exemple les droits inhibés A'0, B'0.

Une opération de comparaison D est ensuite effectuée entre les droits actifs (par exemple, A1, B1) contenus dans le module clé C3 et les droits inhibés (par exemple, A'0, B'0) contenus dans le fichier de

déclaration INH.

Si aucun des droits actifs n'est présent dans le fichier de déclaration INH, l'exécution du logiciel est alors autorisée (étape E).

En revanche, si l'un au moins des droits actifs est présent dans le fichier de déclaration INH, le module clé de travail C3 est désactivé (étape F).

Lorqu'un module clé a été désactivé, celui-ci devient inutilisable pour l'exécution d'un logiciel protégé, pour toute opération d'union ou de partition de droits. Les seules opération autorisées sont les opérations de lecture par le logiciel de gestion de droits afin d'identifier les causes qui sont à l'origine de la désactivation du module clé. Ainsi, le prestataire des logiciels, en lisant le contenu du module clé désactivé, est en mesure de prouver qu'il y a eu tentative frauduleuse d'usurpation de droits d'utilisation de logiciels protégés.

L'efficacité du procédé de protection selon l'invention repose sur les nombreuses possibilités de diffusion massive au sein des sites utilisateurs du fichier de déclaration INH. En effet, ce fichier, qui ne peut être lu par le client du fait qu'il est sous forme binaire, peut être diffusé intégralement :

- à chaque livraison d'une nouvelle version de logiciel protégé ou de logiciel de gestion de droits,
- à chaque diffusion de fichiers contenant la mise à jour d'informations descriptives de symboles.

Ce fichier INH est diffusé partiellement :

- par retour à l'utilisateur d'un nouveau module clé après panne (ce nouveau module clé comporte des droits A'o et B'o en plus des droits A1 et B1, en remplacement des droits Ao et Bo),
- à l'occasion de toute opération d'union ou de partition effectuée par recopie des droits inhibés

éventuels en plus de la recopie des droits actifs objets de l'opération,

- lors d'un transfert d'un module clé contenant des droits inhibés, du poste de travail initial vers un autre poste de travail, ces droits inhibés étant alors inscrits dans le fichier INH du nouveau poste de travail,

- à chaque mise en oeuvre d'un nouveau logiciel protégé.

Bien sûr, la présente invention n'est pas limitée aux exemples qui viennent d'être décrits et de nombreux aménagements peuvent être apportés à ces exemples sans sortir du cadre de l'invention.

Ainsi, le procédé selon l'invention peut s'appliquer à de nombreux types de postes de travail , pourvu qu'ils soient dotés d'un support de clés. Il peut aussi s'appliquer à la protection de logiciels exploités sur des automates programmables.

En outre, le procédé n'est pas limité au cas particulier de deux logiciels qui vient d'être décrit et peut bien sûr être appliqué à un grand nombre de logiciels dans la limite de capacité du poste de travail hôte. On peut aussi envisager d'autres types de support d'informations numériques qu'une disquette, par exemple des supports magnéto-optiques ou des microcircuits.

REVENDICATIONS

1. Procédé de protection des droits d'utilisation d'un ou plusieurs logiciels sur un poste de travail informatique ou d'automatisme industriel (1, 10), ces droits étant contenus dans un module clé de travail (C1, C3) destiné à coopérer avec le poste de travail (1, 10) pour autoriser une continuité d'exploitation desdits logiciels, caractérisé en ce qu'il comprend, en cas de panne du module clé de travail (C1), une phase de contrôle de la détention effective par l'utilisateur du poste de travail (1, 10), des droits (A0, B0) dont la restitution est demandée, ledit module clé de travail (C1) et chacun desdits droits d'utilisation (A0, B0) étant initialement associés respectivement à un identificateur de clé et à des identificateurs de droit d'utilisation et en ce qu'il comprend en outre, au cours de toute exécution de l'un au moins desdits logiciels ou transaction portant sur lesdits droits d'utilisation, une opération d'enregistrement de l'identificateur de clé et des identificateurs de droit d'utilisation dans au moins un fichier prédéterminé (CLE, FUS) accessible sur le poste de travail (1, 10) et transmis sur un support d'informations numériques (F1) avec le module clé de travail (1,10) défaillant.

2. Procédé selon la revendication 1, caractérisé en ce que la phase de contrôle comprend une étape de mise à jour (a) d'un fichier client (FC) comprenant notamment les identificateurs de clé et de droit d'utilisation, une étape de mise à jour (b) d'un fichier de déclaration (INH) contenant l'ensemble des droits d'utilisation déclarés détruits par l'ensemble des utilisateurs desdits logiciels, et une étape (c) de préparation et de retour au client d'une part, d'un nouveau module clé de travail (C3) contenant des nouveaux droits d'utilisation (A1, B1) des logiciels, auxquels sont associés de nouveaux

identificateurs de droit, et les droits d'utilisation des logiciels, qui ont été déclarés détruits et qui sont maintenant inhibés (A'0, B'0), et d'autre part, un support d'informations numériques (F3) contenant notamment le fichier de déclaration (INH) sous une forme non accessible en lecture, notamment sous forme binaire, en vue de charger ledit fichier (INH) sur le poste de travail (1,10).

3. Procédé selon la revendication 2, caractérisé en ce qu'il comprend en outre, préalablement à l'exécution de l'un desdits logiciels protégés ou d'un logiciel de gestion de droits d'utilisation, les étapes suivantes:

A/ lecture de l'ensemble des droits d'utilisation (A0, B0; A1, B1, A'0, B'0) contenus dans le module clé de travail (C1, C3),

B/ remise à jour d'un fichier de clé (CLE) contenant l'identificateur de clé et les identificateurs des droits d'utilisation initiaux, nouveaux et inhibés contenus dans le module clé de travail,

C/ vérification de l'existence et de l'intégrité au sein du poste de travail (1,10) d'un fichier de déclaration (INH) non accessible en lecture, suivie d'une remise à jour dudit fichier (INH) avec les droits inhibés (A'0, B'0) éventuellement contenus dans le module clé de travail (C3) et préalablement lus dans l'étape A/,

D/ comparaison des droits d'utilisation actifs (A0, B0; A1, B1) contenus dans le module clé de travail (C1, C3) avec l'ensemble des droits inhibés contenus dans le fichier de déclaration (INH), conduisant, si aucun des droits actifs n'est présent dans ledit fichier (INH), à l'exécution (E) du logiciel concerné, et dans le cas contraire, à une désactivation (F) du module clé de travail (C3).

4. Procédé selon la revendication 3, caractérisé

en ce qu'une version remise à jour du fichier de déclaration (INH) est régulièrement diffusée auprès des utilisateurs des logiciels protégés, notamment lors de la fourniture de versions nouvelles de logiciels de gestion de droits d'utilisation ou de logiciels utilitaires associés aux logiciels protégés.

5. Procédé selon l'une des revendication 3 ou 4, caractérisé en ce qu'au cours d'une opération d'union-partition de droits contrôlée par un logiciel de gestion de droits d'utilisation et impliquant un premier module clé (C3) contenant des droits actifs et des droits inhibés et un second module clé (C4), les droits inhibés lus dans le premier module clé (C3) sont dupliqués dans le second module clé (C4).

6. Procédé selon l'une des revendications 3 à 5, caractérisé en ce que le déplacement d'un module clé de travail (C3) d'un premier poste de travail (1) auquel elle était initialement associée à un second poste de travail (10) conduit à la remise à jour du fichier de déclaration (INH) associé à ce second poste de travail (10) avec les droits inhibés contenus dans le module clé de travail (C3).

7. Système (40) de protection des droits d'utilisation d'un ou plusieurs logiciels sur un poste de travail informatique ou d'automatisme industriel (1,10), ces droits étant contenus dans un module clé de travail (C1,C3) destiné à coopérer avec le poste de travail (1,10) pour autoriser une continuité d'exploitation desdits logiciels, mettant en oeuvre le procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comprend des moyens (41) pour contrôler la détention effective par l'utilisateur du poste de travail (1,10), de droits (A0, B0) dont la restitution est demandée en cas de panne du module clé de travail (C1), à partir d'informations contenues dans des fichiers

prédéterminés (CLE, FUS) remis par l'utilisateur sur un support d'informations numériques (F1) avec le module clé de travail défaillant (C1), notamment un identificateur de clé associé audit module clé et des identificateurs de droits d'utilisation associés respectivement à chacun des droits d'utilisation (A0, B0) initialement présents dans ledit module clé (C1).

8. Système (40) selon la revendication 7, caractérisé en ce que les moyens de contrôle (41) comprennent des moyens pour mettre à jour, d'une part, un fichier client (FC) contenant notamment l'identificateur de clé et les identificateurs de droit d'utilisation, et d'autre part, un fichier de déclaration (INH) contenant l'ensemble des droits d'utilisation déclarés détruits par l'ensemble des utilisateurs desdits logiciels, des moyens pour configurer un nouveau module clé de travail (C3) contenant des droits nouveaux (A1, B1) d'utilisation des logiciels, auxquels sont associés de nouveaux identificateurs de droit, et les droits d'utilisation qui ont été déclarés détruits et qui sont maintenant inhibés (A'0, B'0), et des moyens pour générer sur un support d'informations numériques (F3) retourné à l'utilisateur des logiciels avec le nouveau module clé de travail (C3), le fichier de déclaration (INH) sous forme non accessible en lecture en vue de charger ledit fichier (INH) sur le poste de travail (1, 10).

9. Système (40) selon la revendication 8, caractérisé en ce que les moyen de génération sont agencés pour générer en outre le fichier de déclaration (INH) sur un support d'informations numériques (F3) comportant un fichier (SYM) contenant des informations descriptives de symboles, notamment de symboles commerciaux.

10. Système (40) selon l'une des revendications 8 ou 9, caractérisé en ce que les moyens de configuration

sont agencés pour configurer deux nouveaux modules clés de travail contenant chacun plusieurs couples constitués d'un droit d'utilisation et de son droit correspondant déclaré détruit inhibé, lorsque le module clé de travail en panne contenait initialement des droits d'utilisation en nombre supérieur ou égal à une valeur limite prédéterminée.

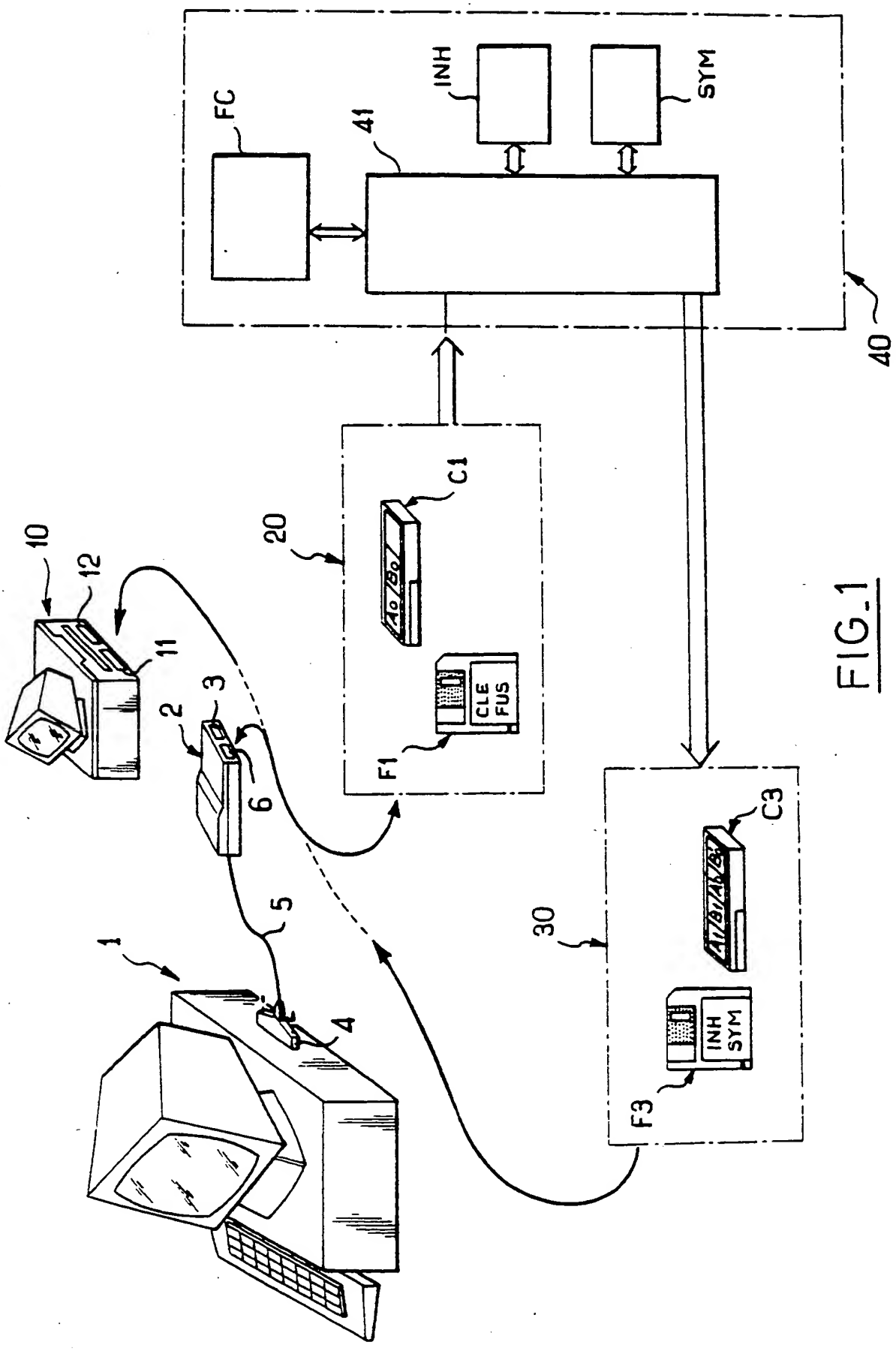


FIG_1

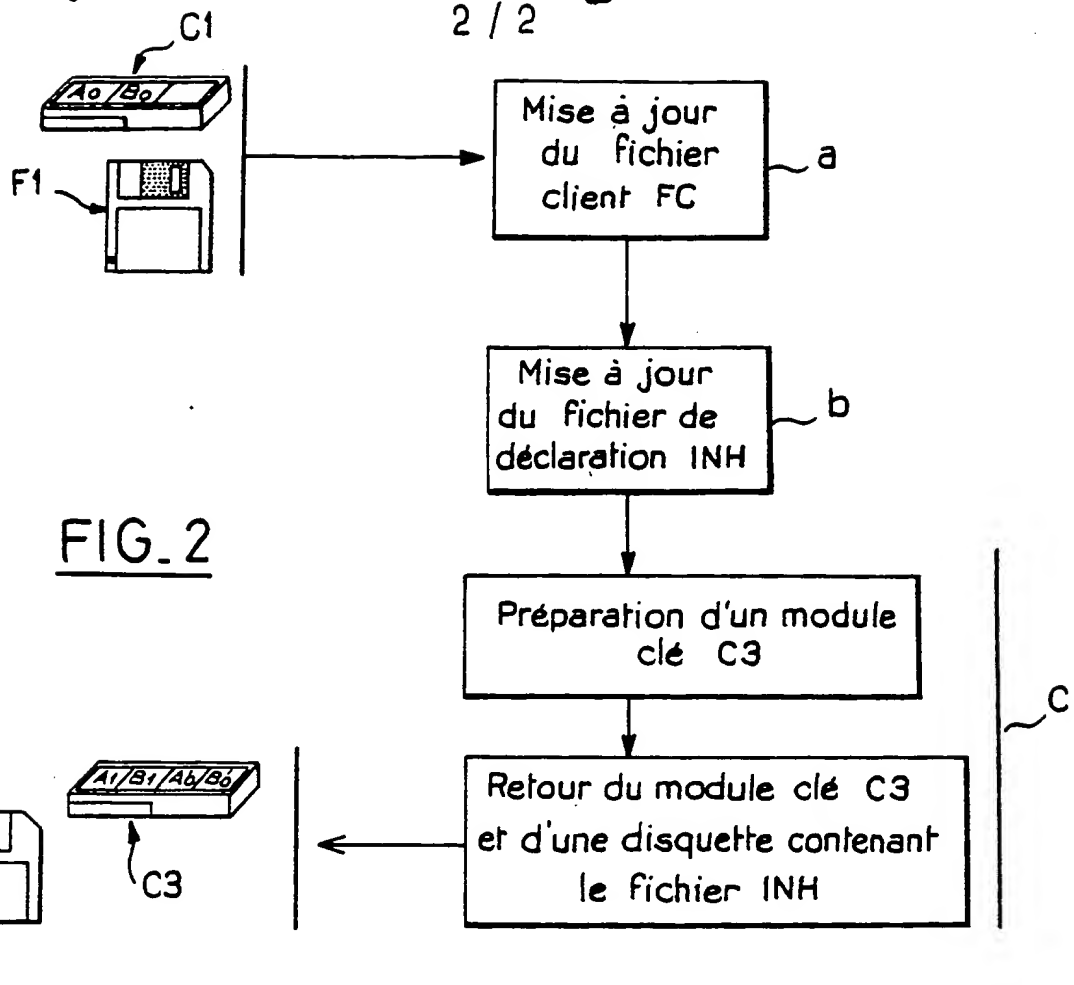


FIG_2

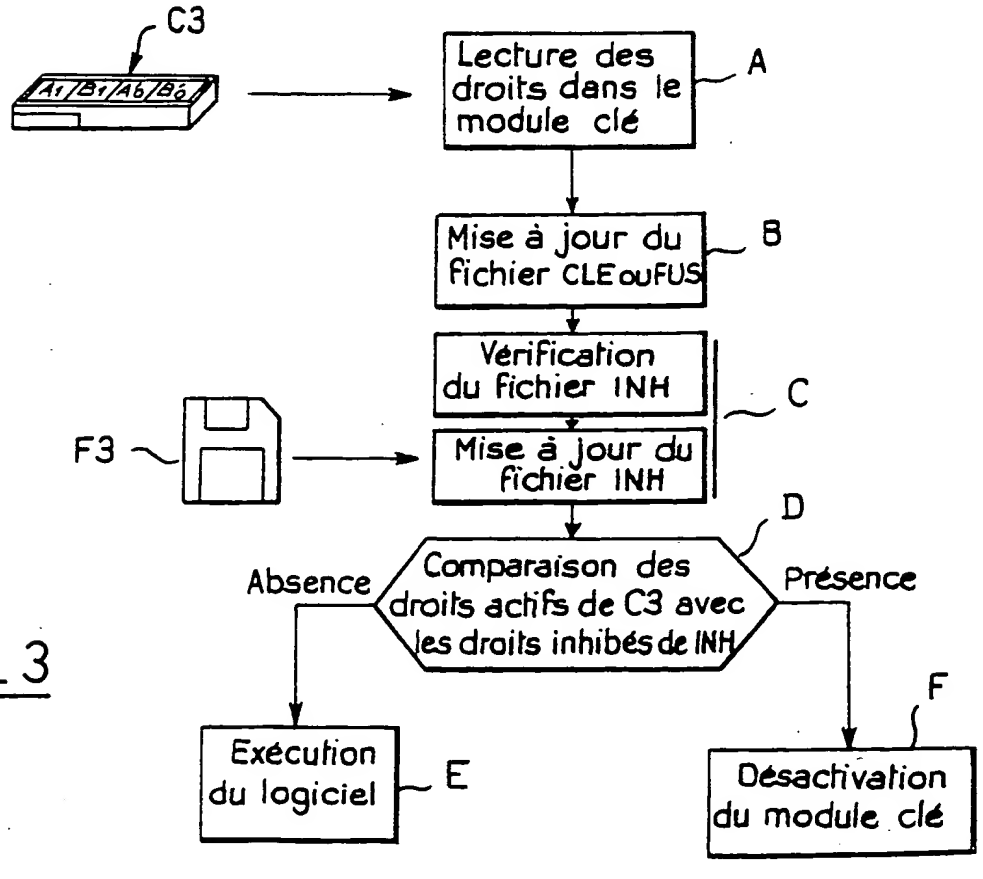


FIG_3

REPUBLIQUE FRANÇAISE

2667173

N° d'enregistrement national

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

FR 9011675
FA 448586

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
A	EP-A-0 268 139 (IBM) * Colonne 10, ligne 32 - colonne 11, ligne 23; colonne 12, lignes 5-17; colonne 29, ligne 6 - colonne 30, ligne 9; figure 17 * -----	1,7

DOMAINES TECHNIQUES RECHERCHES (Int. Cl.5)
G 06 F 1/00

Date d'achèvement de la recherche	Examinateur
22-02-1991	MOENS R.A.A.

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P0413)